REMARKS

Reconsideration of the rejections set forth in the Office action dated 12/31/2003 is respectfully requested under the provisions of 37 CFR §1.111(b).

Claims 1-24 were pending.

Claims 22, 23 and 24 are canceled.

No claims were amended.

I. *Drawings*

After receiving an office action for companion case 09/596,857 where the Examiner of that case noticed that figures 1A, 1B, and 1C were missing, the Applicant reviewed the instant case and has determined that the same figures are missing.

Applicant's current attorney of the instant case prepared an affidavit for the attorney of case 09/596,857. A copy of this affidavit is included herewith. Applicant's attorney for application 09/596,857 provided the following remarks (where the citations have been updated for the instant application).

> ...After a review of our files, applicant believes that Figures 1A-1C were not sent with the application by the patent firm who wrote this application. Applicant includes herewith a proposed drawing correction that includes the missing figures. Figure 1B is described in the specification at page 12, lines 2-11. Figure 1C is described in the specification at page 11, lines 13-22. No new matter was added by the proposed Figures 1B and 1C as the text clearly describes what these proposed figures show. Thus, proposed Figure 1B and 1C simply conform to the specification.
>
> Figure 1A is described starting at page 9, line 31 through page 11, line 2 -- and in the context established at page 8, line 23 through page 9, line 31. Applicant's current attorney assigned the task of recreating Figure 1A to another patent attorney, Mr. Daniel B. Curtis, reg: 39,159. According to Mr. Curtis' affidavit filed herewith, Mr. Curtis read the specification, and prior to discussing the issue with the inventors, used the specification and his own understanding of the technology to conceptualize the cryptoserver architecture. Mr. Curtis reduced

his conceptualization to proposed Figure 1A and verified his conceptualization of the system architecture with Inventor Smetters. Mr. Curtis is no more than skilled in the art. Thus, no new matter was added by proposed Figure 1A because the proposed figure is supported either directly or inherently, by the originally filed specification, drawings, or claims as interpreted by one skilled in the art and because proposed Figure 1A merely clarifies or completes the original disclosure.

As the disclosure for the instant application related to Figure 1A is slightly different from the disclosure of Figure 1A in application 09/596,857, applicant's attorney has added identifying request handler threads as element 156, and the reply as element 162.

Applicant's current attorney for the instant application (Mr. Curtis) also believes that no new matter is added by Figures 1A, 1B, and 1C and respectfully requests that Figures 1A, 1B, and 1C be approved and entered in the instant case.

I. Amendments to the specification

The amendments to the specification are not believed to add new matter, but were made to correct typographical errors and to improve the clarity of the disclosure.

II. General Comments regarding the claimed invention

The applicant believes that the Examiner may not fully understand some of the context of the invention. In particular, the applicant would like to point out to the Examiner that the claimed invention is directed towards pricing a **cryptographic service**. The cryptographic service is described at page 15, line 19 through page 16, line 4; page 19, lines 13-19; and page 20, lines 17-22.

To summarize, a cryptographic service provider operates a cryptographic server. The cryptographic server provides cryptographic services to clients such that the client can off-load the computational burden related to a cryptographic operation from the client computer to the cryptographic server that provides the service of performing the cryptographic operation. The client pays for the requested cryptographic service (page 21, lines 1-5). One example of such a cryptographic service is that of encrypting data provided by the client (page 19, lines 27-31). Another example is that of performing

modular exponentiation (page 16, lines 27-31). Thus, instead of a client computer performing the cryptographic operation, the client sends a request to a cryptographic server that determines the price of the requested service and performs the requested cryptographic service for the client.

The cryptographic service is thus a service provided by a cryptoserver that off-loads the computational burden due to cryptographic operations from a client computer. The pricing of this service is important as the operator of the client computer needs to be able to determine the cost of using the cryptographic service.

The cryptographic service is completely different from the technology provided by the cited art. In particular, as will be discussed below, none of Nakamura (that encrypts and sends real-time data to a receiver that decrypts the encrypted data --- for example cable or satellite video), Iwamura (accounting for an information distribution system), Billstrom (anonymous access to a communication network), and Jakobsson (mix networks), separately or combined teach or suggest a cryptographic service as that term is used in the instant application.

III. Rejections under 35 USC § 102(b)

Claims 1, 4, 5, 8, 11, 12, 15, 18 and 19 were rejected under 35 USC § 102(b) as being anticipated by Nakamura (5,159,633).

A prima facie case of anticipation is established when the Examiner provides a single reference that teaches or enables each of the claimed elements (arranged as in the claim) expressly or inherently as interpreted by one of ordinary skill in the art.

Applicant respectfully traverses this rejection to the claims as a prima facie case has not been established.

Looking first at Nakamura.

The problem addressed by Nakamura is that of securely providing real-time data (such as video).

In a first embodiment, Nakamura teaches methods for securely communicating a secret-key using public-key cryptography between a source and a receiver such that a real-time data stream can be encrypted at the source using the secret-key and securely transmitted to a receiver where the secret-key is used to decrypt the real-time data stream. Nakamura also teaches a payment system for providing the real-time data as a function of size of the real-time data. This embodiment is similar to pay-for-view video using cable or satellite.

In a second embodiment, Nakamura teaches methods for using the disclosed technology for providing video conferencing.

In both embodiments, Nakamura first uses public-key encryption to exchange a secret-key that can be used to encrypt and decrypt real-time information.

Turning now to the invention of original claim 1 is directed to a cryptoserver and is a method for pricing a cryptographic service, comprising:

(a) receiving a request for the cryptographic service;

(b) identifying a computational burden required to perform the cryptographic service, including one or more of a privacy level of the cryptographic service or a speed of performing the cryptographic service; and

(c) determining a price of the cryptographic service based on the at least one of the computational burden, privacy level, and speed.

Thus, the claimed invention is directed to pricing a requested cryptographic service.

Nothing in Nakamura would teach or enable determining a price for a cryptographic service because Nakamura teaches nothing about providing a cryptographic service as that term is used in the instant application.

The office action asserts that Nakamura discloses receiving a request for a cryptographic service (step (a) above) citing column 7, lines 1-4. However, the cited text does not teach a request for a cryptographic service. This text states that Nakamura uses a public-key system to encrypt and transmit information needed to perform the real-time encryption of the requested real-time data. One skilled in the art would not consider this citation or any other portion of Nakamura as teaching a request for a cryptographic service (such a request being, for example, a request to perform cryptographic work that is off loaded from a client).

The office action asserts that Nakamura column 9, lines 55-63 teach steps (b) and (c) above. However, although Nakamura measures the time required to encrypt and decrypt the information encrypted using the secret-key and uses that measurement to determine the charge access to the information, this does not teach step (b) above because the Nakamura does not provide a cryptographic service for the reasons previously stated.

Thus, original claim 1 is not anticipated by Nakamura.

Original claim 8 is directed to a computer program that, when executed by a computer, causes the computer to perform the method of claim 1. Thus, claim 8 is not anticipated for the same reasons as original claim1 is not anticipated.

Original claim 15 is directed to a system that contains logic to perform the method of claim 1. Thus, claim 8 is not anticipated for the same reasons as original claim1 is not anticipated.

Claims 4, 11, and 18 depend on and further limit their respective parent claims and thus are also not anticipated. In addition, Nakamura does not teach or enable a cryptographic service.

Claims 5, 12 and 19 depend on and further limit their respective parent claims and thus are also not anticipated. Applicant respectfully points out that Nakamura teaches absolutely nothing about Private Information Retrieval which would be understood by one skilled in the art at the time of the invention to mean technology that allows a user to retrieve a record of his/her choice from a database server such that nobody (not even the

server) observes the identity of the record. Research on Private Information Retrieval was started around 1995.

IV. Rejections under 35 USC §103(a)

Claims 2, 3, 9, 10, 16, and 17 stand rejected under 35 USC §103(a) as being unpatentable over Nakamura as applied to claims 1, 8, and 15 and further in view of Iwamura (6,272,535).

A prima facie case of obviousness is established when the Examiner provides one or more references that were available to the inventor and that teach a suggestion to combine or modify the references the combination or modification of which would appear to be sufficient to have made the claimed invention obvious to one of the ordinary skill in the art.

Applicant respectfully traverses this rejection of claims 1, 8, 15, 2, 3, 9, 10, 16 and 17 as a prima facie case was not presented.

With regards to claims 1, 8, and 15, nothing in Nakamura suggested the need for a cryptographic service or the need to price the cryptographic service. The problem addressed by Nakamura is that of securely providing real-time data (such as video) not that of off-loading the burden of cryptographic calculations from a client to a cryptographic server that provides a requested cryptographic service. Nothing in Nakamura would suggest a cryptographic service or the need for pricing a cryptographic service to one skilled in the art. Thus, original **claims 1, 8 and 15** are patentable.

Turning now to Iwamura.

Iwamura teaches multiple ways to deliver and charge for providing information. The fourth embodiment teaches a user specifying the level of encryption that is to be applied to the information prior to delivery and being charged accordingly. Like Nakamura, Iwamura does not provide a cryptographic service (as that term is used in the

present application) but simply provides a mechanism for providing data that has been protected by a user-selected level of encryption.

With regards to claims 2, 3, 9, 10, 16 and 17, these claims depend on and further their respective parent claims that are patentable. Thus **claims 2, 3, 9, 10, 16 and 17** are patentable. In addition, neither Nakamura nor Iwamura separately or combined teach a suggestion to off-load the burden of cryptographic calculations from a client to a cryptographic server that provides a requested cryptographic service or the need for pricing the cryptographic service.

Claims 6, 13 and 20 stand rejected under 35 USC §103(a) as being unpatentable over Nakamura as applied to claims 1, 8, and 15 and further in view of Billstrom (5,729,537). Applicant respectfully traverses this rejection of claims 1, 8, 15, 6, 13, and 20 as a prima facie case of obviousness was not presented.

Billstrom teaches group authentication.

With regards to claims 1, 8, and 15, nothing in Nakamura suggested the need for a cryptographic service or the need to price the cryptographic service. The problem addressed by Nakamura is that of securely providing real-time data (such as video) not that of off-loading the burden of cryptographic calculations from a client to a cryptographic server that provides a requested cryptographic service. Nothing in Nakamura would suggest a cryptographic service or the need for pricing a cryptographic service to one skilled in the art. Thus, original **claims 1, 8 and 15** are patentable.

With regards to claims 6, 13, and 20 these claims depend on and further their respective parent claims that are patentable. Thus **claims 6, 13 and 20** are also patentable. In addition, nothing in Nakamura nor Billstrom separately or combined teach a suggestion to off-load the burden of cryptographic calculations from a client to a cryptographic server that provides a requested cryptographic service or the need for pricing the cryptographic service.

Claims 7, 14, and 21 stand rejected under 35 USC §103(a) as being unpatentable over Nakamura as applied to claims 1, 8, and 15 and further in view of Jakobsson

(6,049,613). Applicant respectfully traverses this rejection of claims 1, 8, 15, 7, 14, and 21 as a prima facie case of obviousness was not presented.

With regards to claims 1, 8, and 15, nothing in Nakamura suggested the need for a cryptographic service or the need to price the cryptographic service. The problem addressed by Nakamura is that of securely providing real-time data (such as video) not that of off-loading the burden of cryptographic calculations from a client to a cryptographic server that provides a requested cryptographic service. Nothing in Nakamura would suggest a cryptographic service or the need for pricing a cryptographic service to one skilled in the art. Thus, original **claims 1, 8 and 15** are patentable.

Jakobsson teaches mix networks.

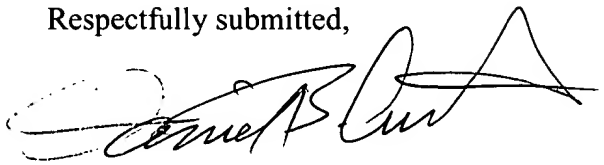
With regards to claims 7, 14, and 21 these claims depend on and further their respective parent claims that are patentable. Thus **claims 7, 14 and 21** are also patentable. In addition, nothing in Nakamura nor Jakobsson separately or combined teach a suggestion to off-load the burden of cryptographic calculations from a client to a cryptographic server that provides a requested cryptographic service or the need for pricing the cryptographic service.

No additional fee is believed to be required for this amendment. However, the undersigned Xerox Corporation attorney hereby authorizes the charging of any necessary fees, other than the issue fee, to Xerox Corporation Deposit Account No. 24-0025. This also constitutes a request for any needed extension of time and authorization to charge all fees therefor to Xerox Corporation Deposit Account No. 24-0025.

Since all rejections, objections and requirements contained in the outstanding official action have been fully answered or traversed and shown to be inapplicable to the present claims, it is respectfully submitted that reconsideration is now in order under the provisions of 37 CFR §1.111(b) and such reconsideration is respectfully requested. Upon reconsideration, it is also respectfully submitted that this application is in condition for allowance and such action is therefore respectfully requested.

Should any additional issues remain, or if I can be of any additional assistance, please do not hesitate to contact me at (650) 812-4259.

Respectfully submitted,



Daniel B. Curtis
Attorney for Applicants
Reg. No. 39,159
(650) 812-4259
dbcurtis@parc.com